Terminus System

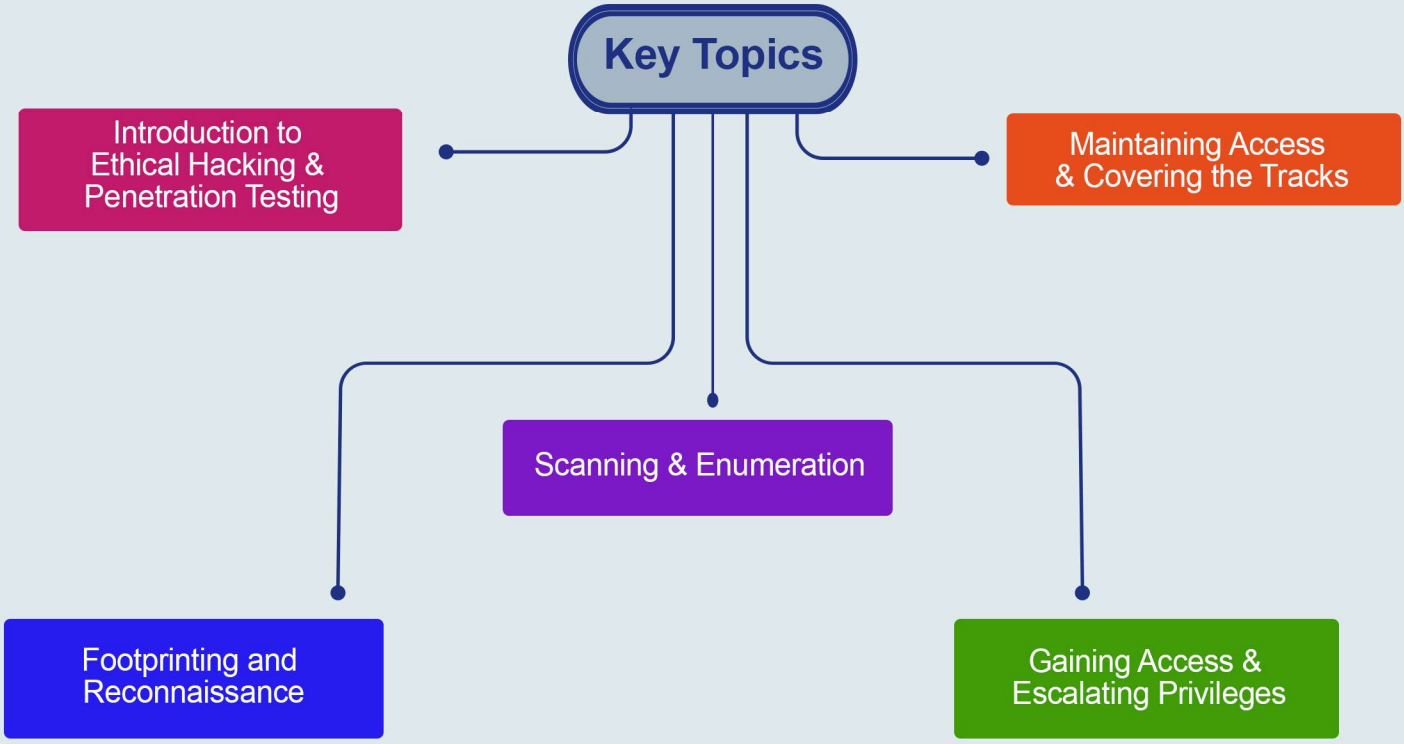
About the Course

This course will immerse you into the Hacker Mindset so that you will be able to defend against future attacks. The security mindset in any organization must not be limited to the silos of a certain vendor, technologies or pieces of equipment. This ethical hacking course puts you in the driver's seat of a hands-on environment with a systematic process. Here, you will be exposed to an entirely different way of achieving optimal information security posture in their organization; by hacking it! You will scan, test, hack and secure your own systems. You will be taught the five phases of ethical hacking and the ways to approach your target and succeed at breaking in every time! The five phases include Reconnaissance, Gaining Access, Enumeration, Maintaining Access, and covering your tracks.

Learning Objectives

1. Understanding Concepts of Ethical Hacking and Penetration Testing
2. Familiarity with Different Penetration Testing Methodologies
3. Penetration Test Planning
4. Familiarity with Different Phases of Penetration Testing
5. Performing Ethica Hacking & Penetration Testing
6. Penetration Test Reporting

Key Topics



Pre Requisites

A basic understanding of networking, operating systems, services, products, and protocols, information security and information security management topics is mandatory for students attending this class. It is also necessary to take the following courses:

- InformationSecurity Concepts & Principles
- Network Securiity

Terminus System

What You Will Receive

- Course Presentation File
- Complementary Files
- Ethical Hacking & Penetration Testing Concepts eBook

Who Should Attend

Anybody who is in charge of security assessment and penetration testing and also:

- CISOs
- PenTesters
- Threat & Vulnerability Analysts
- Security Specialists

Syllabus

Introduction to Ethical Hacking

- Ethical Hacking Terminology
- Ethical Hacking Concepts
- Methodologies

Penetration Testing

- Penetration Testing Benefits
- Types of Penetration Testing
- Penetration Testing Methodologies
- Penetration Testing Planning & Scheduling
- Pre-Penetration Testing Checklist
- Penetration Testing Reporting

Footprinting and Reconnaissance

- Footprinting Concepts
- Footprinting Methodology
- Footprinting through Search Engines
- Google Search
- Google Hacking
- GHDB
- Footprinting through Web Services
- Footprinting through Social Networking Sites
- Website Footprinting
- Email Footprinting
- Whois Footprinting
- DNS Footprinting
- Network Footprinting
- Footprinting through Social Engineering
- NNTP Newsgroups & Information Leakage from Mail Headers
- Footprinting Countermeasures

Syllabus

Scanning

- Scanning Overview
- Scanning Tools
- Host Discovery and Live System Scanning Techniques
- Port & Service Discovery
- Active and Passive Operating System Fingerprinting
- Banner Grabbing
- Determining Firewall Filtering Rules & IDS Evasion Techniques
- Scanning beyond IDS and Firewall
- Vulnerability Scanning
- CGI Scanning
- Network Diagram Drawing
- Proxies & Anonymizers
- IP Spoofing
- Finding Trust Relationship in Active Directory
- How to Steal Wireless Profiles
- User Behavioral Analytics

Enumeration

- Enumeration Concepts & Overview
- NetBIOS & SMB Enumeration
- SNMP Enumeration
- LDAP Enumeration
- NTP & NFS Enumeration
- DNS Enumeration
- MYSQL Enumeration
- MSSQL Enumeration
- SMTP Enumeration
- Enumeration Countermeasures

Syllabus

System Hacking

- Gain Access
- Esclating Priviledges
- Executing Applications

Maintaining Access

- Backdoors
- Trojan horse
- Rootkits
- Kernel-Level Rootkits

Covering the Tracks

- File and Directory Camouflage and Hiding
- Log File Editing
- Accounting Entry Editing
- Covert Channels over HTTP, ICMP, TCP, and other Protocols
- Sniffing Backdoors
- Steganography

Hands-on Training

- Lab 1 - Footprinting Through Search Engines
- Lab 2 - Footprinting Through Web Services
- Lab 3 - Footprinting Through Social Networking Sites
- Lab 4 - Website Footprinting
- Lab 5 - Email Footprinting
- Lab 6 - Whois Footprinting
- Lab 7 - DNS Footprinting
- Lab 8 - Network Footprinting
- Lab 9 - Host Discovery
- Lab 10 - Port and Service Discovery
- Lab 11 - OS Discovery
- Lab 12 - Scan Beyond IDS and Firewall
- Lab 13 - Draw Network Diagrams
- Lab 14 - Network Scanning Tools
- Lab 15 - NetBIOS Enumeration
- Lab 16 - SNMP Enumeration
- Lab 17 - LDAP Enumeration
- Lab 18 - NFS Enumeration
- Lab 19 - DNS Enumeration
- Lab 20 - RPC, SMB and FTP Enumeration
- Lab 21 - Vulnerability Research
- Lab 22 - Vulnerability Assessment Tools
- Lab 23 - Gain Access to the System
- Lab 24 - Perform Privilege Escalation to Gain Higher Privileges
- Lab 25 - Maintain Remote Access and Hide Malicious Activities
- Lab 26 - Clear Logs to Hide the Evidence of Compromise
- Lab 27 - Gain Access to the Target System using Trojans